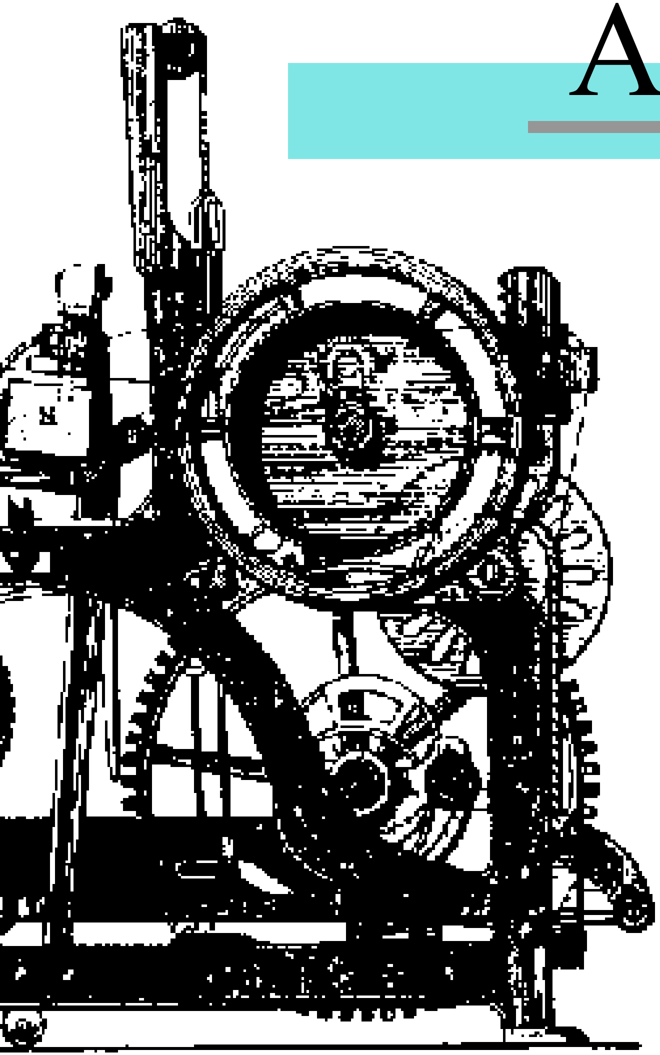
Reshaping Key Management: A Tale of Two Decades



John Iliadis, University of the Aegean, 2000

De Facto Joint Research Group on Information and Communication Systems Security

Overview

- Communication Networks: Now and Then.
- New Key Management Paradigm
- Certificates
- Certificate Management
- Intro to TTPs and PKI

Communication Networks: Now and Then

- Then
  - Centralised
  - Closed
    - private or semi-private, no access allowed,
    - wide spectrum of proprietary networking/communication protocols,
    - expensive,
    - targeted user group,
    - early Internet instances.

Communication Networks: Now and Then (cont.)

- Now
  - Distributed
    - no ownership,
    - no central control,
    - resilience.
  - Open
    - access to anyone,
    - standardised protocols,
    - low-cost access.

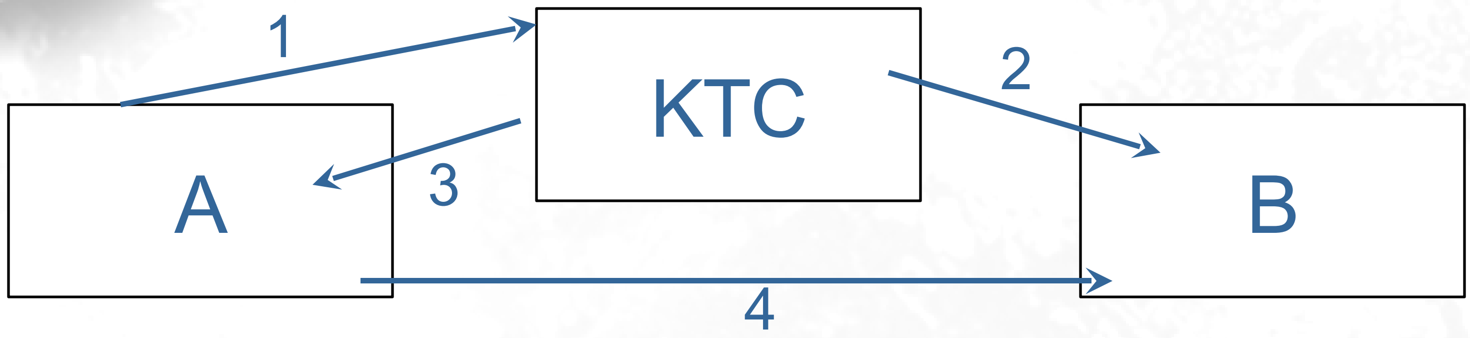
Basic Services of Key Management

- Generate-Key
- Register-Key
- Create-Key-Certificate
- Distribute-Key
- Install-Key
- Store-Key
- Derive-Key
- Archive-Key
- Revoke-Key
- Deregister-Key
- Destroy-Key

Key Distribution - Symmetric Cryptosystems

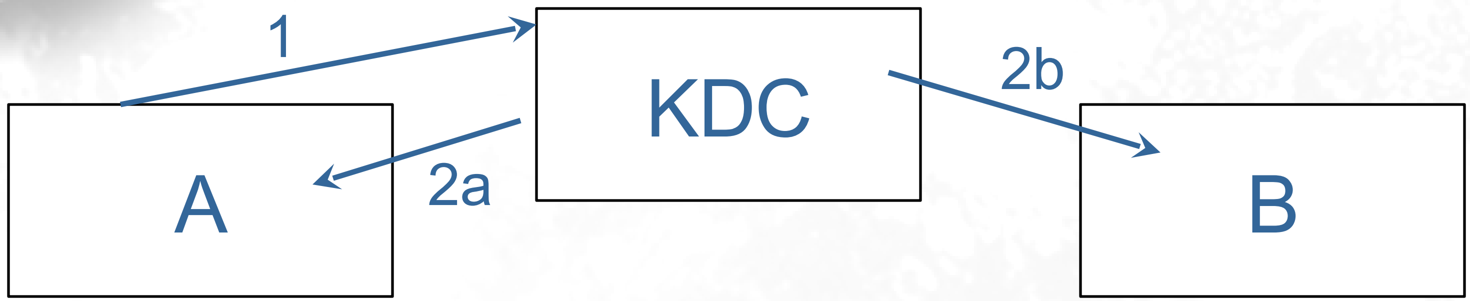
- Direct
- Key Translation Center
- Key Distribution Center
- Based on asymmetric techniques
  - secret key agreement
  - secret key transport

Key Translation Center (symmetric crypto)



- A->KTC: enciphered key
- KTC->B: sends B re-enciphered key, **OR**
- KTC->A: sends A re-enciphered key
- A->B: A sends B re-enciphered key

Key Distribution Center (symmetric crypto)



- A->KDC: request for shared key
- KDC->A: sends A enciphered shared key
- KDC->B: sends B enciphered shared key

If KDC cannot communicate securely with B (2b), then A assumes responsibility for distribution of enciphered shared key to B

Key Distribution in Symmetric Cryptosystems - A Note

- All mechanisms require the existence of a shared symmetric or asymmetric key and an inline Key Center.

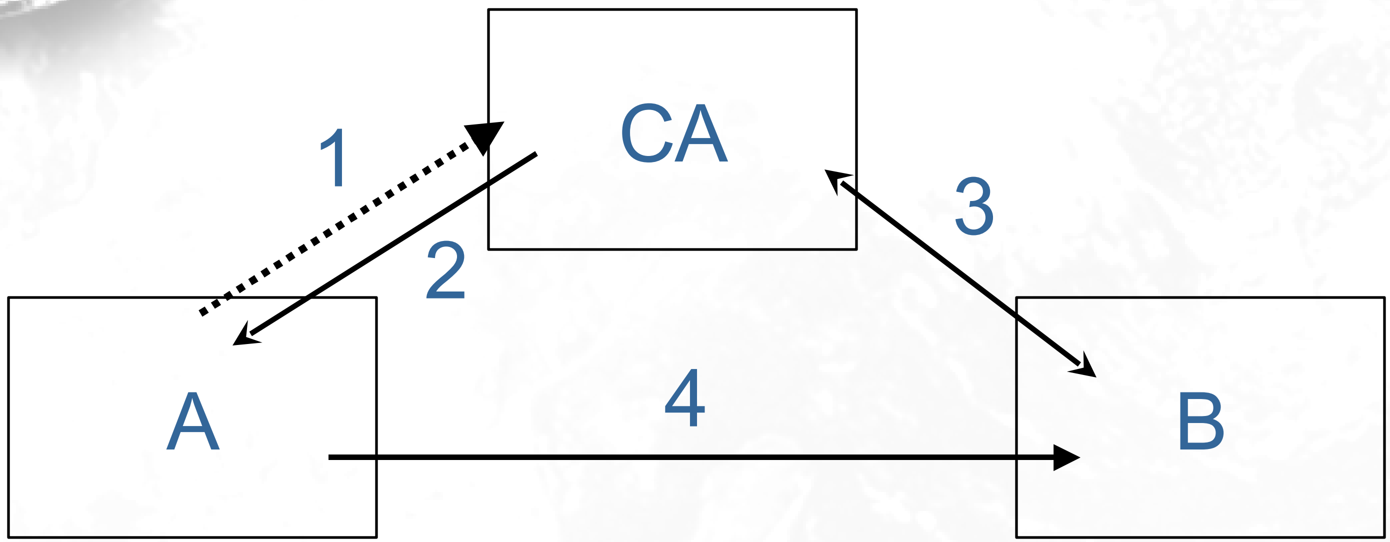
Centralised
Closed
Private
Proprietary protocols
Expensive

Distributed
No ownership
No central control
Resilience
Access to anyone
Standardised protocols
Low-cost access.

Key Distribution - Asymmetric Cryptosystems

- Protected channels (data origin authentication and data integrity protection, e.g. courier and registered mail)
- TTP-assisted (i.e. certificates)

Key Distribution - Asymmetric Cryptosystems (cont.)



- A->CA: Key$_A$ (?)
- CA->A: Certificate$_A$
- CA<->B: Certificate$_A$
- A->B: Certificate$_A$

Key Distribution in Asymmetric Cryptosystems - A Note

- Mechanisms require the existence of either an integrity protected channel, or an (at least) offline TTP*

Centralised
Closed
Private
Proprietary protocols
Expensive

Distributed
No ownership
No central control
Resilience
Access to anyone
Standardised protocols
Low-cost access.

*Other TTP operational requirements, like revocation, necessitate the online operation of TTPs

Key Distribution - A Final Note

- The Case of Asymmetric versus Symmetric Cryptosystems, and vice-versa.
  Verdict: *Innocent on all charges*, both of them.
  - there are communications that necessitate symmetric crypto, like small scale closed networks, top-secret communication lines (one-time pads) etc.
  - there are applications that necessitate symmetric crypto, like encryption. Asymmetric encryption is far too slow in most cases, either because of huge amount of data or because of small computational power (e.g. smart cards)

Key Distribution - A Final Note (cont.)

- The Case of Asymmetric versus Symmetric Cryptosystems, and vice-versa.
  Verdict 2: The Case should never have been taken to court!
  - There's no point in excluding or reducing usage of one of them. Joint usage leads to best results (e.g. Digital Envelopes, asymmetric based distribution of symmetric keying material).
  - There are advantages and disadvantages in both. The main difference is in key management requirements: confidentiality against authenticity

Key Distribution - A Final Note (cont.)

Asymmetric crypto was not invented to meet the needs of the new, distributed and loosely federated networking environments. It existed before.

A solution in search of a problem or rather an application area...

Digital Certificates

- Offline authentication token
- Third, trusted entity vouches for it
- Expiration, revocation
- Contents:
  - identification info of certificate holder
  - identification info of CA
  - public key of certificate holder
  - expiration date
  - other info (e.g. CSI location info)
  - signed by CA

Digital Signatures

- Generating certificate-supported signatures
- Non-repudiation
  - Timestamping
  - Non-repudiation mechanisms and fair exchange mechanisms
  - Underlying legal framework

European Directive on Electronic Signatures

- Directive aims at technology independence
- Problem: Directive identifies requirements that fall under the scope of technology (e.g. secure signature creation devices, Annex III)
- Solution: Define sets of components that comply with the Directive. Caution needed when defining these sets; they must not conflict with other, underlying regulatory frameworks

Secure Signature Creation Devices

- Hardware tokens
  - easier to deploy
  - wide acceptance by public as a «secure» method
  - degree of security awareness required: low
- Security requirements and evaluation standards
  - harder to deploy; compliance certification (end-user systems)?
  - degree of public confidence: low
  - degree of security awareness required: high

Secure Signature Creation Devices (cont.)

- Factors to consider:
  - Ease of use,
  - confidence/acceptance by public,
  - cost of implementation, operation and maintenance,
  - security level and assurance,
  - others...

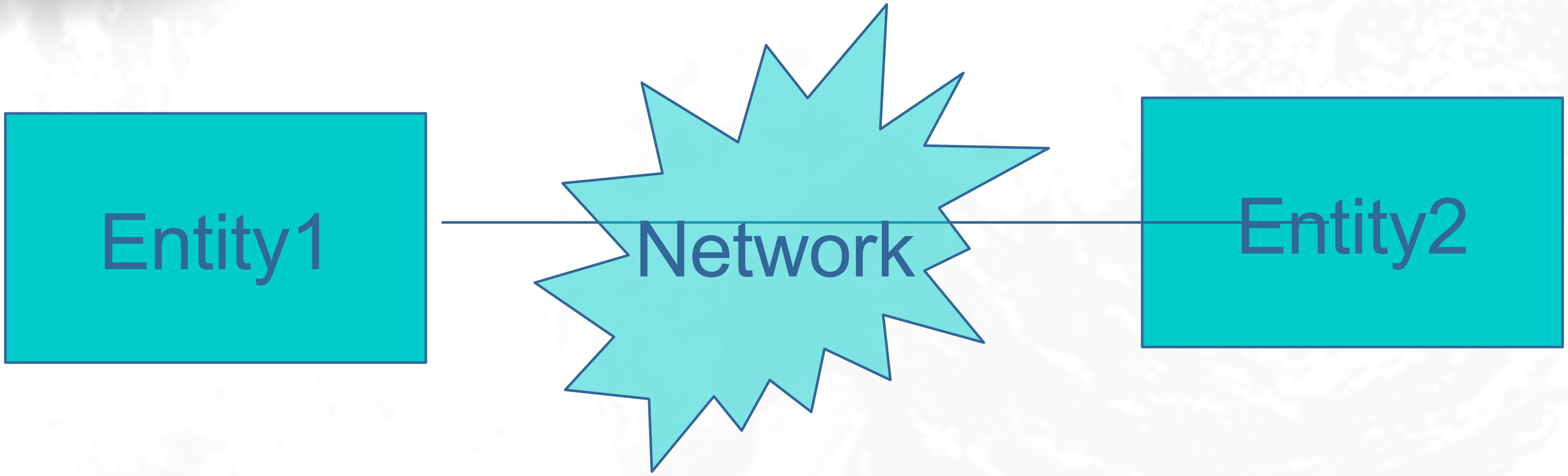
Main Points in Certificate Lifecycle

- Key generation
- Entity Registration
- Certificate Distribution
- Certificate Archiving
- Revocation

Some Threats in Electronic Transactions

- Monitoring of communication lines
- Shared key guessing/stealing
- Shared key stealing
- Unauthorised modification of information in transit
- Masquerade - Web spoofing
- Password stealing
- Unauthorised access

Insecure Electronic Transactions



Facing Threats

- *monitoring of communication lines*
  Encryption with randomly generated shared session key
- *shared session key stealing/guessing*
  -cryptographically secure random key generators
  -encryption of shared session key with the public key of the receiving entity
- *Non-authorised modification of (in-transit) information*
  secure hashing algorithms for message authentication codes

Facing Threats

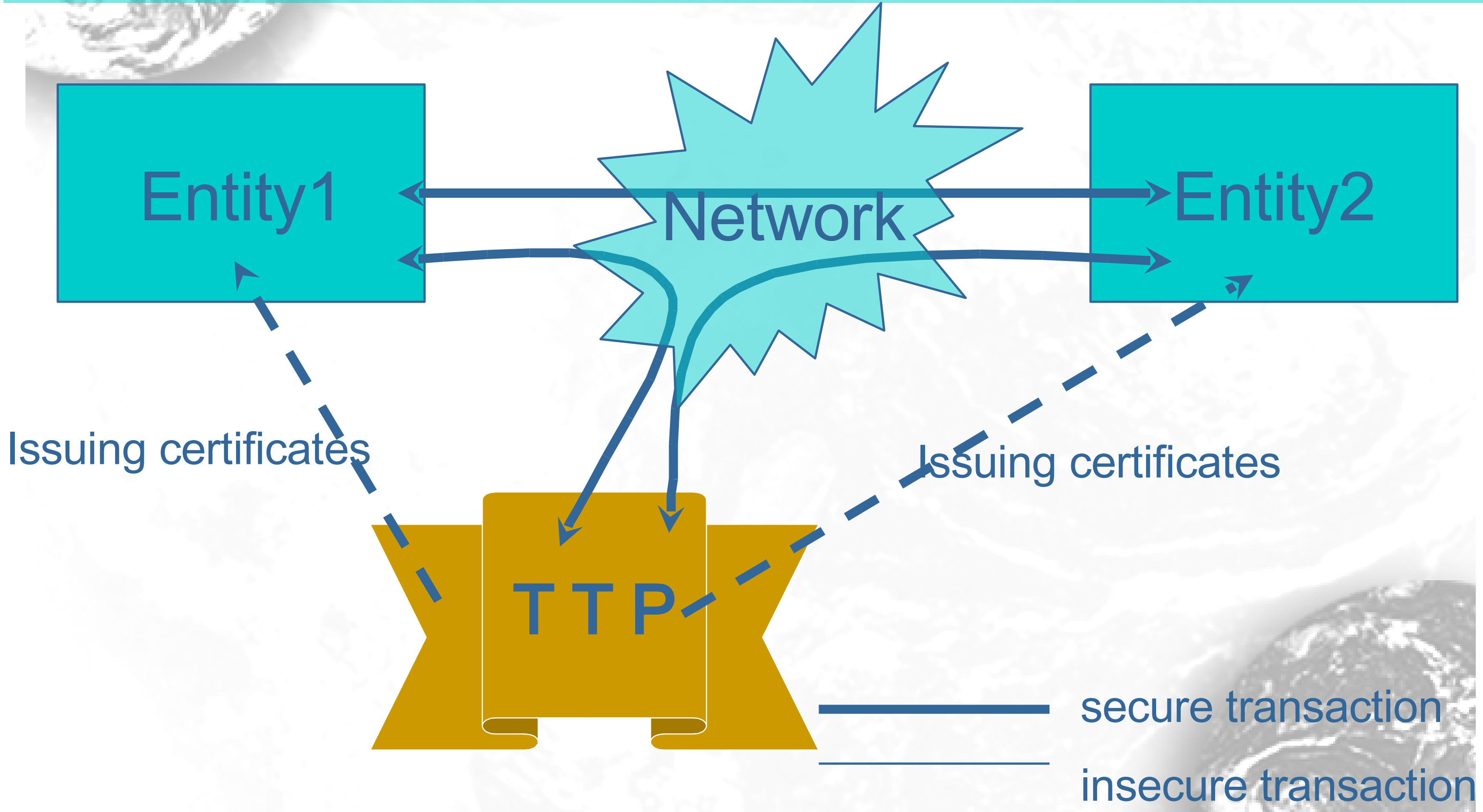
- *Masquerade - Web spoofing*

  Exchange of X509v3 certificates and verification against a Directory
- *Password stealing*

  Passwords are never transmitted in the network
- *Unauthorised access*

  Local ACL. Authentication by certificate verification

Securing electronic transactions



TTP : The Cornerstone of a Public Key Infrastructure. An Overview

TTP : “an impartial organisation delivering business confidence, through commercial and technical security features, to an electronic transaction”

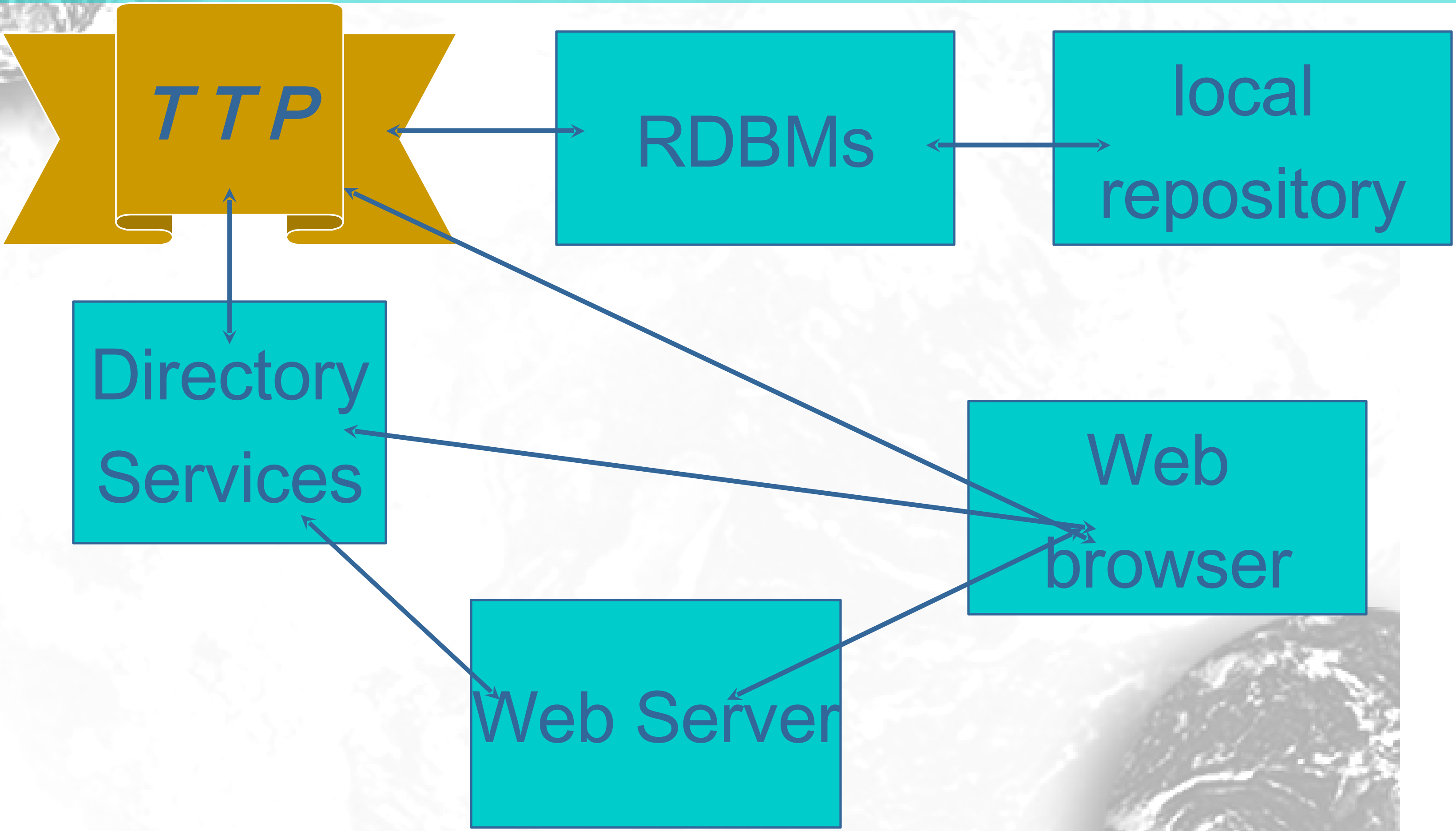
TTP : The Cornerstone of a Public Key Infrastructure.

Technical Infrastructure

- *Certificate Authority,* providing certificates.
- *Registration Authority*, registering users and binding their identities to certificates.
- *Repositories,* storage and dissemination entities containing TTP-related public material such as certificates and CRLs.
- *Certificate holders,* holding certificates from CAs which they use in order to sign or authenticate themselves.
- *Dependent entities,* entities which use the certificates presented by other entities in order to authenticate the latter or verify their signature.

TTP : The Cornerstone of a Public Key Infrastructure.

Technical Infrastructure



PKI

- Set of TTPs
- Interoperability and corroboration
- Legal framework
- Value-Added services
  - Timestamping
  - Information Archiving
  - Notary Public
  - ...

Fashion Issues concerning PKI

- Current commercial PKI trends
  - It’s fashionable
  - It’s easy to deploy…Typical installations of TTP software, withour prior analysis of requirements and without designing a Security Policy and a Certificate Policy, are not that far. It happened (is happening?) with firewalls some time ago...
  - It meets several security requirements, through a wide set of security services ranging from confidentiality to public notary
  - It’s a panacea!

Fashion Issues concerning PKI (cont.)

- **…however:**
  - PKI is nor a cure-all, neither a magical solution to security problems
  - Requirements->Services->Functions ->Implementation
  - Certificate and Security Policy of TTP
  - Legal framework and regulations
  - Complexity in design and development
  - User-awareness needed
  - Clearly not an InfoSec bandage

Conclusion

- PKI is a panacea for security as much as aspirin is a panacea for pain.

Easing ulcer pains with aspirin
SHOULD BE AVOIDED AT ALL COSTS...

Areas needing further research

- Identification and naming.
- Certificate path validation.
- Signature policy.
- Scalable revocations and scalable suspensions.
- Role of notaries.
- Trusted archival services.
- Use of biometrics in relation to electronic signatures.

Some interesting problems to be studied

Certificate 1	**Certificate 2**
John Doe	John Doe
org: X	org: Y
org unit: Xu	org unit: Yu
Country: GR	Country: GR

- In general, TTP service-level collaboration has to be studied further
  - cross-certification (technical, legal)
  - revocation
  - ...

References

- Branchaud M., "A Survey of Public Key Infrastructures", Msc Thesis Department of Computer Science McGill University, Montreal, 1997.
- Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, 13 December 1999, published in the Official Journal of the European Communities, 19 January 2000.
- Housley R., Ford W., Polk W., Solo D., Internet X.509 Public Key Infrastructure Certificate and CRL Profile, , IETF Network Working Group, Request for Comments 2459 (Category: Standards Track), January 1999, available at http://www.ietf.org/rfc/rfc2459.txt
- ISO Standard 11770 (1996), Information Technology - Security Techniques - Key Management - Part 1: Framework.
- ITU-T Recommendation X.509 (1997) and ISO/IEC 9594-8:1997, Information technology - Open Systems Interconnection, "The Directory: Authentication framework".
- Kohnfelder L., Towards a practical public-key cryptosystem, BSc Thesis, M.I.T., Cambridge MA, September 1978.
- Ronald L. Rivest, Adi Shamir, Leonard M. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, vol21, No2, pp.120-126, 1978.
- Schneier B., Applied Cryptography, 2nd ed, John Wiley & Sons, 1996.
- W. Diffie, M. E. Hellman, New Directions in Cryptography, IEEE Transactions, vol IT-22, pages 644-654, 1976.